JON W. FULLINWIDER
CHIEF INFORMATION OFFICER

Telephone: (213) 974-2008
Facsimile: (213) 633-4733

August 24, 2004

To: Supervisor Don Knabe, Chairman
        Supervisor Gloria Molina, Chair Pro Tem
        Supervisor Yvonne B. Burke
        Supervisor Zev Yaroslavsky
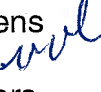   Supervisor Michael D. Antonovich

From: Jon W. Fullinwider
        Chief Information Officer

        Violet Varona-Lukens
        Executive Officer
        Board of Supervisors

Subject: **REPORT ON HALL OF ADMINISTRATION NETWORK OUTAGE AND SOFTWARE PROBLEMS**

On August 10, 2004, your Board directed the Executive Officer and the Chief Information Officer (CIO) to investigate and report back on the cause of the network and e-mail disruptions that occurred around the week of July 26, 2004 at the Kenneth Hahn Hall of Administration (HOA). The motion also requested a description of the steps to be taken to prevent future outages, an assessment of service vendor's response and a plan to allow users to continue to access their local workstations in the event that the e-mail or network systems are not operational.

A team was established, comprised of staff from the CIO, ISD, Executive Office and Cisco Systems. The team has reviewed the documented problems (trouble tickets) reported between July 22, 2004 and August 10, 2004 from the Executive Office's Information Resource Management (IRM) Help Desk, ISD's Customer Assistance Center (CAC), and Cisco System's (Cisco) Technical Assistance Center (TAC). The team also reviewed the system alert logs from the e-mail servers and the network switches. A brief electronic survey was also sent to the Information Technology Managers of HOA departments to understand the scope and impact of the outages among the HOA tenants during the outage. The Countywide Computer Emergency

Response Team (CCERT) issued an advisory to departments indicating a high risk level of activity for the "W32/Mydoom.o@mm" and "W32.Mydoom.m@mm" mass-mailing worms on July 26, 2004. We ruled out the possibility that this cyber-threat contributed to HOA network outage.

Summary of Findings

The investigation team concluded that:

- The network outage experienced at the HOA was caused by a previously unknown hardware defect in network related equipment.

- All equipment in the HOA has been assessed and we have determined that the network is not susceptible to future outages due to this particular hardware problem.

- Cisco's support during the period following our call to their Technical Assistance Center was timely and acceptable in their response.

- No evidence was reported that corroborates a failure with any server managed by the Executive Office's IRM.

- This incident does highlight the need to begin planning an upgrade of the Hall of Administration's network before Cisco terminates support for the hardware and software.

- The Executive Office has been testing the Microsoft Outlook 2003 software which includes improved functionality for offline access to e-mail and calendars. This capability will be implemented following the completion of testing and some end-user training.

It is important to note that network outages cannot be prevented entirely. However, some steps to improve resiliency have already been taken, and others are planned.

Network Incident Review

Our review disclosed that the network problems began on July 22, 2004 and spanned a period until August 4, 2004 before the problems were fully corrected The problems involved a network switch located on the third (3rd) floor that distributes data to and from the individual workstations in the Assessor's and Treasurer & Tax Collector's (TTC) offices at the HOA. ISD's network engineers responded promptly and after a few attempts to diagnose and correct the problem, determined that the problem was caused by a hardware failure. The hardware failure was isolated to an uplink module device within the switch that connects the switch to the fiber optic cables that are the backbone

of the network. The engineers replaced the defective part with a new part from a reserve of spare components maintained by ISD. At that time, the problem appeared corrected (i.e., network operations appeared normal). However, the problem re-occurred the following morning. Hoping to mitigate further downtime while performing additional diagnostics on the cause of the intermittent outages, ISD created an alternate communication route to the building's network "core" (the nexus that connects each switch to other switches within the HOA and to the County's Enterprise Network outside the building). This alternate communication route is called a "dual home" connection. This appeared to temporarily abate the problem. ISD continued monitoring the situation throughout that weekend. During the weekend, all operations appeared to be normal.

On Monday morning, July 26, 2004, ISD noted that connectivity problems between the Assessor and TTC were once again occurring. ISD immediately opened a trouble ticket with Cisco for assistance in resolving this problem. Unbeknownst to ISD, numerous departments throughout the HOA, including the Assessor, TTC, County Counsel, Executive Office, and Consumer Affairs, as well as satellite offices, were experiencing fluctuating connectivity to network resources such as e-mail, calendars, etc. In addition, the Executive Office's IRM, unaware of any network issues that might impact them, rebooted the e-mail servers with hopes of correcting the e-mail communication problem reported by its users.

Despite ISD's and Cisco's efforts, problems still existed at the close of business on July 26, 2004. At 5:00 p.m. ISD identified an unusually high utilization of 98% in the critical building network core switches lending them to believe that the network problem may have been associated with a denial of service virus attack (the CIO's Security Officer had subsequently concluded that there was not a virus attack). ISD also noted that much of the network traffic was associated with the "dual home" connection ISD had installed on the switch on July 22, 2004. ISD disabled the redundant connection which immediately corrected the problem associated with the high utilization.

On the morning of July 27, 2004, some connectivity problems reappeared. From this point through August 4, 2004, ISD and Cisco continued diagnostic work while also implementing work-arounds to enable some level of network connectivity during this timeframe. On August 2, 2004, the root cause of the problem (i.e., Cisco identified a manufacturer's defect in the installed version of the switch's uplink module). A newer version of the part was ordered and installed and the problem was corrected.

Vendor Support

July 26, 2004 was the day when the network problems were the most widespread at the Hall of Administration. Cisco's engineers were providing support consistently from the time they were contacted. As illustrated above, this was a difficult problem to diagnose and Cisco worked diligently with ISD to attempt to correct the problem, including providing another Cisco 5500 switch to replace the switch on the third floor, which was

originally thought to be the source for the larger network problems. Cisco performed continued testing and research. The engineers ultimately found that the new uplink modules that they were installing were a version with a manufacturer's defect, which was the actual source of the problems. Cisco provided replacements for the defective uplink modules with a later version of the components and that has proven to be a reliable correction of the problems.

Additionally, Cisco reviewed the County's current level of support with the company, and agrees that it is sufficient and complete. ISD reports no grievances with Cisco support services and recommends that the County continue its support agreement with Cisco, which proved critical in resolving this recent outage.

E-mail/Calendar Server Review

During the period when the HOA experienced a network outage, there were no problems isolated to the Board of Supervisors' Microsoft Exchange e-mail/calendar servers that caused a separate outage.

On Friday afternoon, July 23, 2004, the Executive Office received a Help Desk call reporting problems accessing e-mail and calendars. Following evaluation by the Executive Office's IRM, it became clear that there was a network problem. The problem was resolved by ISD on a network switch at approximately 7:00 p.m. that night. There was no separate outage that occurred with the Board's Exchange servers.

On Monday morning, July 26, 2004, workstation users reported problems again to the Executive Office. These problems did not manifest themselves on other servers managed by the Executive Office. The Executive Office's IRM initially consulted with staff from ISD. ISD staff indicated that they did not see problems on our building's network. IRM staff then consulted with their Exchange server maintenance vendor. The vendor researched similar problems and based on the assumption that the network was up and operational, recommended that a corrective patch be applied to the Exchange server. This particular patch is not generally available to the public and is only recommended for specific problems. Although the Board's I/T system appeared to operate properly once the patch was installed, the problem returned within 30 minutes. Soon after the patch was applied, ISD informed the Executive Office that they discovered a network malfunction involving the core switches. All logon and slowness problems with the Exchange system were corrected when that problem was remedied. Since then, the Executive Office reports that access to the Board's Exchange system has been operating in a normal, routine manner.

The user perception of the duration of the e-mail and calendar access problems may have extended longer than the actual network outage. The network generated interruption in accessing the e-mail and calendar server could have required users to log off the server and re-logon to re-establish the connection even after the network was

fully operational and the e-mail server was accessible. If staff did not perform this log-off/logon procedure, this could have had a dramatic impact on the perceived duration of the outage.

Actions and Recommendations

The following actions and recommendations are based on the findings from the team's investigation of the recent outages.

Steps Taken to Prevent Similar Outages

In order to further improve its support of the Hall of Administration's network, ISD already has taken the following actions:

- Surveyed all the network equipment in the Hall of Administration to verify that no other devices are at similar risk.

- Initiated actions with Cisco to replace all spares of the uplink module that failed with the manufacturer's recommended version.

- Subscribed to Cisco's "Bug Toolkit" for enhanced searches for known bugs and their resolutions and to Cisco's "Product Alert Tool" for receiving e-mail updates about reliability, safety, network security, and end-of-sale issues for equipment.

- Expanded the retention of system logs from the network equipment on the HOA network management console, in addition to the central logging maintained at the ISD Network Control Center (NCC).

Additionally, ISD is already making changes to the building network infrastructure to increase its resiliency. All of the building's network closets have been surveyed to determine the ability to support "dual-homing", a network configuration where each departmental switch has a redundant path to the building's network core. The necessary hardware has been installed in the core switches, and work is being performed to supplement the building's fiber backbone that connects the departmental switches to the core switches. Although this added redundancy would not have prevented the outage recently experienced, it will increase general network availability. There are sufficient funds already budgeted in ISD's network maintenance budget for these actions and no additional funding is required.

Network Upgrade

The team also identified the need to upgrade the network equipment in the Hall of Administration. The project that implemented the HOA network was completed in 1998. The main class of network switches used throughout the building, the Cisco Catalyst

5500 series, has already entered its end-of-life phase. Cisco, the manufacturer, stopped taking orders for that model in June 30, 2003. Software support is scheduled to end on June 30, 2006 and hardware support will end on June 30, 2008. ISD and CIO will prepare a complete proposal for your consideration within 90 days. Part of that proposal will be a recommendation for a structured plan to provide technology refreshes in order to maintain the viability and sustainability of the Hall of Administration's network.

Offline Access to E-mail/Calendar

The Executive Office's IRM staff is in the process of performing system integration testing prior to upgrading all systems to the Microsoft Windows XP operating system and Microsoft Office 2003. The new office suite package contains upgrades to Microsoft Office Outlook 2003, which includes new capabilities designed to assist in accessing information, such as e-mail and calendars. One of the new features is continued, limited, use of e-mail and calendars when the network becomes unavailable. Outlook 2003 can download mailbox information to the computer, which reduces the need to communicate with the e-mail server. If the network becomes unavailable, Outlook will continue to use the information that has already been downloaded, allowing staff to continue working while the network is down.

The Executive Office's IRM staff will be testing the new version of Outlook for installation and implementation on the Board's computer system. The Department staff will be notified when the migration to the 2003 Outlook occurs, and the ability to access e-mail and calendars during those periods when the network is non-operational. Planning for this upgrade was already in place when the recent network outage occurred.

CIO and ISD staff will be working closely together to develop the network upgrade requirements for the HOA and will be reporting back to your Board in 90 days. Should you have any questions, please contact me at (213) 974-2008.

JWF:JW:DH:ygd

c: County Counsel
        Dave Lambertson, Interim Director, Internal Services Department
        James Hersey, Account Manager, Cisco Systems
        Chair, ISC